UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN RE ASHLEY MADISON CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to: ALL CASES	MDL No. 2669 Case No. 4:15MD2669 JAR

AMICUS CURIAE BRIEF RE: DEFENDANT AVID DATING LIFE INC.'S MOTION FOR PROTECTIVE ORDER

Amici Does 1 through 3 ("Movants") submit the following *amicus curiae* brief in relation to Defendant Avid Dating Life Inc.'s pending motion for a protective order. [D.E. 115.]

I. INTRODUCTION

Amici Does 1 through 3 ("Movants") are former users of the adultery website and dating service operated by Defendant Avid Dating Life Inc. ("Defendant") and known as "Ashley Madison." Movants have been personally affected by the theft by anonymous hackers of massive amounts of private consumer data from Ashley Madison (the "Stolen Data"), which serves as the basis for this multi-district litigation. The Stolen Data includes, among other things, names, passwords, addresses, and phone numbers submitted by Movants and other users of Ashley Madison (collectively, "Consumers") when they registered for and used the website and dating service. The Stolen Data also includes records of millions of credit card transactions dating back to 2008, including cardholder names, billing addresses, associated email addresses, and the last four digits of the credit card number(s) used to pay for each Consumer's account. Movants have already gone to great lengths and expense to protect their privacy by preventing the public dissemination of the Stolen Data, including by initiating legal action against the operators of

websites who repurposed the Stolen Data to make it accessible and searchable by the media and curious Internet users. As a result of this litigation, and other pre-litigation efforts of Movants, the most prominent searchable databases were disabled.

Pending before the Court is Defendant's motion for a protective order prohibiting Plaintiffs or their counsel from using the Stolen Data, which Plaintiffs oppose. Defendant's arguments focus on Defendant's confidential business information and privileged communications with counsel. Plaintiffs, in an attempt to keep the door open for use of the Stolen Data to prove their claims, argue that the Stolen Data is "now fully memorialized in the public domain." (D.E. 130 at 2.) Neither side has briefed the Court on the potential dramatic and negative effects on Consumers if the Court deems the Stolen Data to be in the public domain and therefore legally accessible and/or reproducible.

Movants, together with all other Consumers, have a strong privacy interest in their personally-identifiable and financial information, and this privacy interest should be protected by a protective order. Movants contracted with Defendants to protect this privacy interest. Movants are victims of a crime, where their private consumer records were stolen in violation of numerous federal and state criminal statutes. Now, Movants stand to be re-victimized if the Court adopts the position of Plaintiffs (who purport to represent Movants and all Consumers) that the Stolen Data is within the "public domain."

Accordingly, through this brief, Movants urge the Court to enter a protective order preventing further unlawful dissemination of the 37 million consumer records that are included in the Stolen Data (the "Consumer Records"). Movants do not take a position as to whether any portions of the Stolen Data that do not contain or reference Consumer Records should be subject to a protective order.

II. BACKGROUND

A. Consumer Records Collected by Ashley Madison

In order to use the Ashley Madison dating service, Consumers must register by inputting personally-identifiable information, such as country of residence, zip code, date of birth, email address, and physical attributes, such as height and weight. (Declaration of Karl S. Kronenberger in Support of *Amicus Curiae* Brief ["Kronenberger Decl."] ¶¶3–4, 12–13 & Exs. F–G.) While a Consumer may create an Ashley Madison profile for free, payment is required in order to use any of the services. (*Id.* ¶¶12–14 & Exs. F–H.) Thus, additional personally-identifiable information is collected to process credit and debit card payments, such as credit card number, cardholder name, and associated billing address. (*Id*. ¶14 & Ex. H.)

At various times since 2008, but before July 2015, each Movant registered as a user of Ashley Madison and provided personal and financial information to Ashley Madison in the process. (*Id*. ¶4.) At the time of registration, each Movant reasonably expected that the data provided to Ashley Madison would be managed with sufficient security protocols to prevent hacking or other disclosure. (*Id*. ¶¶5–11 & Exs. A–E.) Like most Consumers, Movants have suffered damages, including severe emotional distress, due to the possibility that their spouses, children, family members, community connections, business associates, and the public at large may identify Movants as users of Ashley Madison. (*Id*. ¶20.) Even now, several months after the theft of this information, Movants and Consumers are inundated with extortionate threats to expose their Ashley Madison information to spouses, family, co-workers, and others. (*Id*. ¶25.)

B. The Stolen Data

In July 2015, a group of hackers, who self-identify as the Impact Team (the "Hackers") released snippets of confidential Consumer information stolen from Defendant's servers, and

then publicly threatened to release much more data if Ashley Madison did not cease operation of its website and dating service. (Kronenberger Decl. ¶18 & Ex. I.) When Defendant refused to cave to the Hackers' demands, on or about August 18, 2015, the Hackers began a rolling release of the Stolen Data. (*Id*. ¶¶18–19 & Exs. I–J.) The Hackers have publicly admitted that the Stolen Data was stolen from Ashley Madison's servers through unlawful hacking. (*Id*.)

The Stolen Data includes, among other things, names, passwords, addresses, and phone numbers submitted by Consumers when they registered for Ashley Madison. (*Id.*) The Stolen Data also includes records of millions of credit card transactions going back to 2008, including the cardholder names, billing addresses, associated email addresses, and the last four digits of the credit card number(s) used to pay for the Consumer's account. (*Id*.) The release of this payment information has been integral to public identification of Consumers in that, while Consumers could falsify personal information, such as by using a fake name, payment information cannot be falsified without the use of a stolen credit card number.

The Hackers' release of the Stolen Data ignited a media frenzy, with news outlets across the globe reporting on it and speculating about politicians and celebrities that could be included within the Consumer ranks. (*Id*.) However, as posted by the Hackers, the Stolen Data is not easily accessed or navigated by the average Internet user. (*Id*. ¶¶16–17, 19 & Ex. J.) The files containing the Stolen Data are each several gigabytes in size, comprise massive strings of plain text, and are posted to the so-called "Dark Web" at an address that is only accessible through the Tor browser. (*Id.*)

C. The Arizona Action

The inaccessibility of the Stolen Data resulted in an overnight cottage industry of websites that took the Stolen Data and reformatted it into databases that could be searched for

specific names, email addresses, billing addresses, or other Consumer information. (Kronenberger Decl. ¶¶15–17, 19 & Ex. J.) In September 2015, Movants filed a lawsuit in the District of Arizona against the operators of the most prominent of these websites, *Doe v. GoDaddy.com, LLC*, Case No. 2:15-cv-01768-DJH (D. Ariz.) (the "Arizona Action"). (*Id*. ¶21.) Movants asserted claims for civil receipt of stolen property under California law, Cal. Pen. Code §496; violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code §17200; intentional and negligent infliction of emotional distress; and violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030—emphasizing the fact that possession of the Stolen Data is no different than receipt of any other stolen good. (*Id*.) Movants reached early resolution with the defendants to disable all access to the reformatted Stolen Data, and thereafter the Movants dismissed the Arizona Action. (*Id*. ¶22.) The Movants, through counsel, have also made multiple pre-litigation legal demands to disable other reformatted versions of the Stolen Data formerly on the Internet. (*Id.*¶23.)

The legal fees for the Arizona Action and other legal efforts to disable the Stolen Data were financed by contributions of over 100 Consumer victims of the Ashley Madison data breach. (*Id.*¶24.) This amicus brief is financed in the same manner. (*Id*.)

D. Defendant's Motion

Movants, and their fellow Consumers, have paid close attention to the developments in the case at hand, which was purportedly initiated to protect their rights. In particular, Movants have reviewed Defendant's Motion for Protective Order Precluding Use of Stolen Documents by Plaintiffs or Their Counsel [D.E. 115] ("Defendant's Motion"), as well as the Plaintiffs'

Opposition to Defendant's Motion [D.E. 130] ("Plaintiff's Opposition").[1] Both of these briefs fail to address the highly sensitive nature of the 37 million Consumer Records that were stolen in the data breach, and how, without protection of this Stolen Data, further distribution will cause significant damage to millions of Consumers.

Shockingly, Plaintiffs state in their Opposition that the "Leaked Documents are in the public domain and therefore may be properly discussed in the pleadings," with Leaked Documents defined as the 30 GB of Stolen Data containing the 37 million consumer records and other business documents. (Opp. at 1, 3 & n.2.) This is particularly disconcerting to Movants, who have fought hard over the past several months to keep the Stolen Data out of the public domain, only to have Plaintiffs' counsel, who are supposedly acting in the interest of the putative class, declare that the Movants' personal Consumer Records are in the "public domain." Movant's position is, and always has been, that the 37 million Consumer Records included in the Stolen Data are not in the public domain, as they are not generally accessible to the public. Further, Movants and other interested Consumers perform daily Internet searches to ensure that no publicly-accessible versions of the Stolen Data have been made available.

Prior dissemination of the Stolen Data has caused incalculable damage to many Ashley Madison Consumers and their families, including divorces and even suicide of some Consumers. For this reason the Movants will continue in their efforts to disable public access to the Stolen Data. However, a ruling by this Court that the 37 million Ashley Madison Consumer Records are in the "public domain," as Plaintiffs argue, would greatly hamper further efforts of the Movants and other Consumers to disable the Stolen Data, as well as provide extortionists and other purveyors of the Stolen Data a legal argument that their actions are not criminal.

[1] Movants have not reviewed the reply of Defendant, which is due concurrent with the filing of this brief, as the Movants did not want to risk the Court ruling on Defendant's Motion prior to considering Movants' request for leave to file its amicus brief.

III. ARGUMENT

A. The Court has the discretion to issue a protective order preventing dissemination or use of the Stolen Data to protect Consumers from annoyance, embarrassment, or oppression.

The Court may issue an order protecting disclosure or discovery upon a showing of good cause. *See* Fed. R. Civ. P. 26(c). For good cause to exist, the parties seeking protection must show that specific prejudice or harm will result if no protective order is granted. *Buehrle v. City of O'Fallon, Mo.*, No. 4:10CV00509 AGF, 2011 WL 529922, at *2 (E.D. Mo. Feb. 8, 2011) (citing *Frideres v. Schiltz,* 150 F.R.D. 153, 156 (S.D. Iowa 1993)). The prejudice or harm protected by Rule 26(c) includes "annoyance, embarrassment, oppression, or undue burden or expense." *Id.* (citing Fed. R. Civ. P. 26(c); *Crawford–El v. Britton,* 523 U.S. 574, 599 (1998)); *see also Gutierrez v. Benavides*, 292 F.R.D. 401, 404 (S.D. Tex. 2013) ("Protective orders are intended to protect these privacy interests and prevent the infliction of unnecessary or serious pain on parties entitled to such protection."). Here, it is undisputable that the inclusion of information within the Stolen Data sufficient to identify Movants and other Consumers presents a substantial risk of annoyance, embarrassment, and oppression. This prejudice outweighs any need of Plaintiffs to access or reproduce in any fashion the Stolen Data, as Plaintiffs do not require the Stolen Data to prove that the data breach took place. Indeed, the Hackers have admitted that they breached Defendant's security protocols. Accordingly, the Court should issue the Protective Order as to the Consumer Records.

//

//

//

B. The Court has the inherent power to issue the requested protective order because the 37 million Consumer Records within the Stolen Data are stolen property.

As noted by Defendant in its brief, which Movants will not restate here, the Court has the inherent power to issue protective orders related to stolen property (Mot. at 4–5, citing *Smith v. Armour Pharmaceutical Co.*, 383 F. Supp. 1573, 1578 (S.D. Fla. 1993); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 568 (S.D.N.Y. 2008); *Fayemi v. Hambrecht & Quist, Inc.* 174 F.R.D. 319, 321 (S.D.N.Y. 1997). Still, perhaps due to the fear of making certain admissions detrimental to its defense, Defendant does not emphasize enough that the Stolen Data constitutes stolen property, the same as if it were a tangible item stolen from a home or storefront.

Plaintiffs' position that stolen property loses its criminal taint through public dissemination is not only unsupported by law, but contradicted by it. The law has worked hard to keep pace with advances in hacking through legislation such as the Computer Fraud and Abuse Act, 18 U.S.C. §1030, the Stored Communications Act, 18 U.S.C. §2701, the Identity Theft and Assumption Deterrence Act, 18 U.S.C. §1028, and updates to wiretapping laws. Knowing receipt of stolen property is a crime in and of itself in all fifty states. *See, e.g.*, Ala. Code § 13A-8-16; Cal. Pen. Code § 496(c); Mo. Rev. Stat. § 570.080; N.Y. Pen. Code § 165.40.

Plaintiffs' apathetic treatment of the Stolen Data as something less than stolen property not only flies in the face of these laws, but calls into question Plaintiffs' adequacy as representatives of Consumers. In at least one jurisdiction, California, there is precedent for courts providing injunctive relief to prevent the dissemination of stolen information, including digital information. *See, e.g.*, *Lynn v. Gateway Unified Sch. Dist.*, No. 2:10-CV-00981-JAM, 2011 WL

6260362, at **2–3 (E.D. Cal. Dec. 15, 2011), *as amended* (Dec. 16, 2011) (recounting related state court case awarding preliminary injunction to prevent dissemination of stolen email communications); *see also, e.g.*, *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (issuing TRO where Muslim advocacy organization would likely suffer irreparable injury from further disclosure of confidential information). Because the Stolen Data was obtained through criminal acts, the Court should prevent any use thereof through the requested Protective Order.

C. The 37 million Consumer Records within the Stolen Data are <u>not</u> within the public domain.

Plaintiffs' so-called "public domain" analysis is not relevant for the purpose of determining whether Movants and Consumers have a legitimate privacy interest in their own Consumer Records and other personal information that was stored on Defendant's servers. The concept of documents being in the public domain is primarily a matter of copyright law to describe copyrightable content that is no longer protectable under copyright law. *See, e.g.*, *Warner Bros. Entm't v. X One X Prods.*, 644 F.3d 584, 595 (8th Cir. 2011) (holding that movie theater's abandonment of the right to control reproduction of publicity materials for *The Wizard of Oz* and *Gone with the Wind* caused such materials to go into the public domain such that no copyright applied). Courts have also used the term, although perhaps inappropriately, to describe trade secrets that have lost their protected status by virtue of being disclosed to the public. *See, e.g.*, *Sigma Chem. Co. v. Harris*, 794 F.2d 371, 375 (8th Cir. 1986) (former employee enjoined from disclosing trade secrets permitted to use that information which is already in the public domain); *see also* Opp. at 4. However, the concept of public domain is not relevant to an analysis of whether a person's privacy interests have been infringed, particularly where the owners of the

information did nothing to waive their privacy rights. *See Chasnoff v. Mokwa*, 466 S.W.3d 571, 579 (Mo. Ct. App. 2015), *transfer denied* (Aug. 18, 2015) (outlining the prima facie elements of invasion of privacy as: (1) publication or publicity, (2) absent any waiver or privilege, (3) of private matters in which the public has no legitimate concern, (4) so as to bring humiliation or shame to a person of ordinary sensibilities).

Notwithstanding the irrelevance of the public domain analysis to whether the Court should protect Movants' privacy rights, the 37 million Consumer Records within the Stolen Data are not in the public domain, as they are not readily accessible by the public given the format and location as released by the Hackers. To get access to the Stolen Data, one must navigate to the so-called "Dark Web," where the Hackers posted the data and which can only be accessed through the Tor browser. (Kronenberger Decl. ¶16.) The Dark Web can be used anonymously, inhibits the ability of law enforcement and others to track users making data available in the Dark Web, and has become a frequent tool of the criminal underworld.[2]

Once one locates the raw data files for the Stolen Data, getting access to it is daunting. The Hackers released the Stolen Data in the form of multiple multi-gigabyte (e.g., 20GB) compressed files that take hours to download and decompress. (*Id.* ¶17.) These files are taken from a series of database backups, and are comprised of massive strings of plain text, as well as 2,642 separate CSV (commas separated value) files containing daily credit card transactions. Many consumer PCs do not have sufficient RAM or hard drive space to save and open any of the separate multi-gigabyte files, and basic text programs preinstalled on PCs cannot open these large files. (*Id*. ¶17.) In order to configure the database backups for ease of use, one needs specialized database administrative skills, software, and knowledge of a database control

[2] *See, e.g.*, Benjamin Weiser & Doreen Carvajal, "International Raids Target Sites Selling Contraband on the 'Dark Web,'" *N.Y. Times*, Nov. 7, 2014, *available at* http://www nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html?_r=1.

language known as SQL. (*Id*.) Once the data from the multiple data sets is loaded into a database, it can only be searched with complex SQL query strings. (*Id*.) Simply put, the format of the Stolen Data released by the Hackers is complex and not accessible by the vast majority of the public.

D. Neither Defendant's Motion nor Plaintiffs' Opposition adequately addresses the need to protect the 37 million Consumer Records in the Stolen Data or explains how Plaintiffs intend to use the Stolen Data.

In its Motion, Defendant requests that the Court "issue a protective order, ordering that neither Plaintiffs nor their counsel may use documents that were stolen from Defendant Avid Dating Live through a hack of its computer system." (Mot. at 14.) While this broad request does cover the 37 million Consumer Records, Defendant's legal argument focuses primarily on stolen business documents, many of which, according to Defendant, are protected by the attorney client privilege or are otherwise confidential. (Mot. at 9–14.)

In their Opposition, Plaintiffs take the extreme view that the "Leaked Documents are in the public domain and therefore may be properly discussed in the pleadings," with Leaked Documents defined broadly as the Stolen Data. (Opp. at 1 and 3, fn. 2.) Plaintiffs also state that "for present purposes, they ***do not intend to use any of the original documents that were leaked in the data breach***," and that "Plaintiffs intend to reference only published news articles, pending further Orders of the Court." (Opp. at 3 & n.2 [emphasis in original].) However, during a phone call with counsel for Plaintiffs on March 22, 2016, counsel for Plaintiffs refused to agree a) that the 37 million private Consumer Records should be protected by a protective order, or b) that they would never use the 37 million stolen Consumer Records. (Kronenberger Decl. ¶26.) Moreover, in the midst of their finger-pointing, neither Plaintiffs nor Defendant address the

privacy rights of Consumers in their highly sensitive and personal information contained within the Stolen Data.

E. Further disclosure of the Consumer Records within the Stolen Data will irreparably injure Movants and other Consumers.

The Movants, along with millions of other Consumers, registered as users of Ashley Madison and provided personal and financial information to Ashley Madison in the process. (Kronenberger Decl. ¶¶4–14, Exs. A–H.) At the time of registration, each consumer reasonably expected that the information provided to Defendant would be kept highly confidential and secure against Hackers. (*Id.*) Involvement on a website that facilitates extramarital affairs is a highly sensitive and confidential matter for virtually anyone engaging in such activity. Thus, Movants and other Consumers had a legitimate expectation of privacy in their data and never intended or anticipated that their information would be made public. For that reason they contracted with Ashley Madison to keep their consumer information confidential. (*Id.* ¶7 & Ex. B.) The Court should protect the 37 million Consumer Records, consistent with the nature of the Ashley Madison consumer agreements and the nature of the private data, in order to protect against further harm through their disclosure.

//

//

//

IV. CONCLUSION

For all of the foregoing reasons, Movants respectfully request that the Court grant Defendant's Motion, at least in part, by issuing a protective order preventing further access, dissemination or use of the Consumer Records within the Stolen Data.

Dated: March 25, 2016

Respectfully submitted,

/s/ Karl S. Kronenberger

Karl S. Kronenberger
CA Bar No. 226112
Virginia Sanderson
CA Bar No. 240241
KRONENBERGER ROSENFELD, LLP
150 Post St., Suite 520
San Francisco, CA 94108
Tel: (415) 955-1155
Fax: (415) 955-1158
Karl@KRInternetLaw.com
Ginny@KRInternetLaw.com

Attorneys for Amici Does 1 through 3

CERTIFICATE OF SERVICE

I hereby certify that on March 25, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing(s) to all counsel of record.

s/ Karl S. Kronenberger
Karl S. Kronenberger